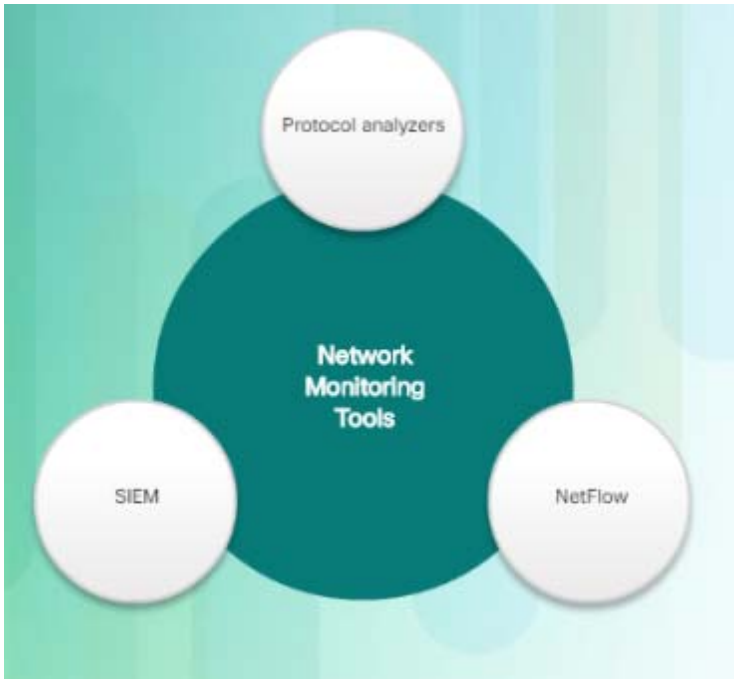
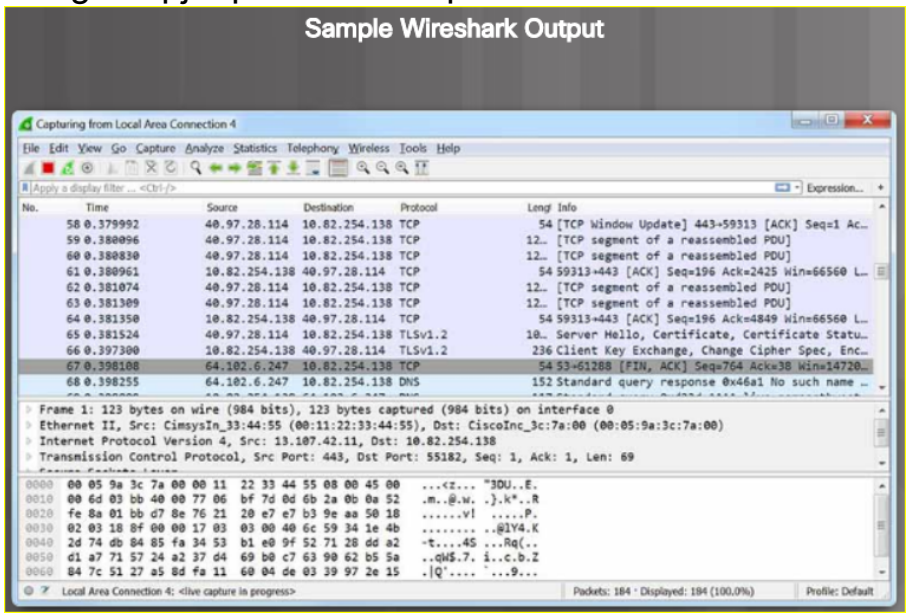
Hyrje në mjetet e monitorimit të rrjetit
Mjetet e monitorimit të sigurisë së rrjetit

- Mjetet e monitorimit:
  - Analizuesit e Protokollit - Janë programet e përdorura për të kapur trafikun? Ex. Wireshark dhe Tcpdump.
  - NetFlow - Ofron një gjurmim të plotë të auditimit të informacionit bazë rreth çdo rrjedhe IP të përcjellë në një pajisje.
  - SIEM - Sistemet e Menaxhimit të Informacionit të Sigurisë japin raportim në kohë reale dhe analiza afatgjata të ngjarjeve të sigurisë.
  - SNMP - Simple Network Management Protocol siguron aftësinë për të kërkuar dhe mbledhur pasivisht informacion në të gjitha pajisjet e rrjetit.
- Dosjet e regjistrit - Gjithashtu është e zakonshme që analistët e sigurisë të kenë qasje në skedarët e logaritjeve Syslog për të lexuar dhe analizuar ngjarjet dhe alarmet e sistemit.

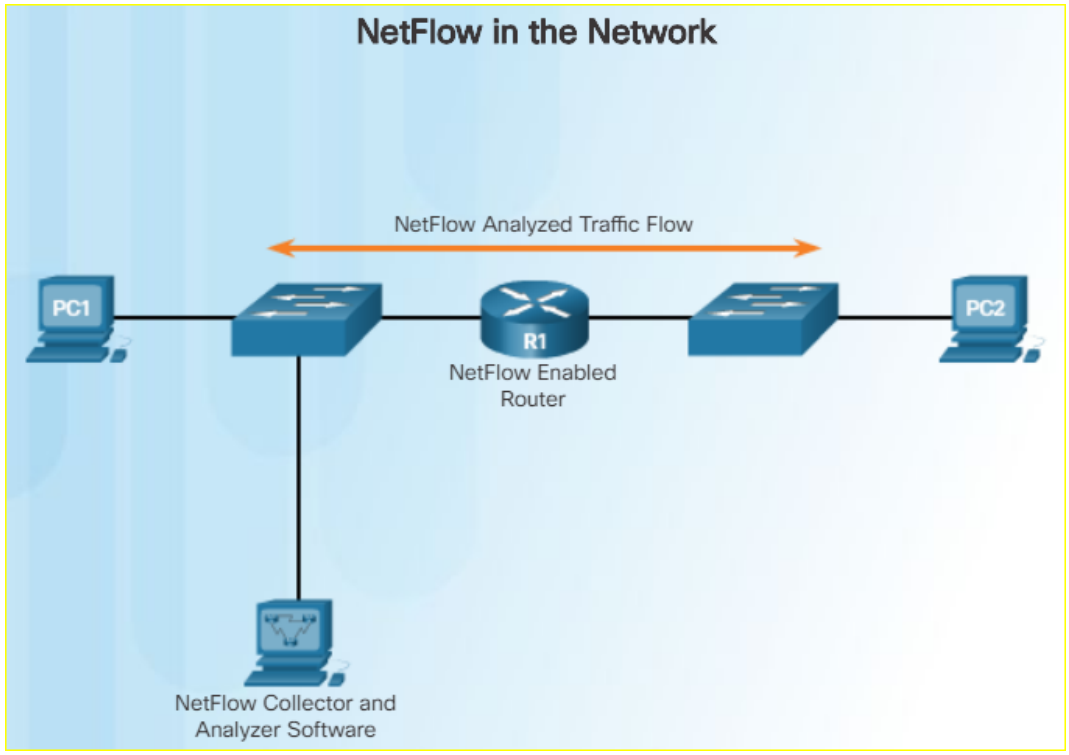


Hyrje në mjetet e monitorimit të rrjetit
Analizatorë të Protokollit të Rrjetit

- Analistët mund të përdorin analiza të protokollit si Wireshark dhe tcpdump për të parë shkëmbimet e rrjetit deri në nivelin e paketës.
- Analizuesit e protokollit të rrjetit janë gjithashtu shumë të dobishme për zgjidhjen e problemeve të rrjetit, zhvillimin e softuerit dhe protokollit, dhe edukimin. Në sigurimin e forenzikës, një analist i sigurisë mund të rindërtojë një incident nga kapjet përkatëse të paketave.



Hyrje në mjetet e monitorimit të rrjetit
NetFlow



- NetFlow është një teknologji e Cisco IOS që ofron statistika 24x7 në pako që rrjedhin përmes një router Cisco ose kalon më shumë nivele.
- NetFlow mund të përdoret për monitorimin e rrjetit dhe sigurisë, planifikimin e rrjetit dhe analizën e trafikut; megjithatë, ai nuk kap përmbajtjen.

Hyrje në mjetet e monitorimit të rrjetit
SIEM

- Sistemet e Menaxhimit të Eventeve të Informacionit të Sigurisë (SIEM) sigurojnë raportim në kohë reale dhe analiza afatgjate të ngjarjeve të sigurisë.
- SIEM përfshin funksionet themelore si në vijim:
  - Analiza mjeko-ligjore - Aftësia për të kërkuar shkrimet dhe regjistrimet e ngjarjeve nga burimet në të gjithë organizatën. Ai jep informacion më të plotë për analizën e forenzikës.
  - Korrelacioni - Ekzaminon shkrimet dhe ngjarjet nga sisteme ose aplikacione të ndryshme, duke shpejtuar zbulimin dhe reagimin ndaj kërcënimeve të sigurisë.
  - Agregimi - Grumbullimi zvogëlon vëllimin e të dhënave të ngjarjes duke konsoliduar regjistrimet e ngjarjeve të dyfishta.
  - Raportimi - Raportimi paraqet të dhënat korresponduese dhe të agreguara të ngjarjeve në monitorimin në kohë reale dhe përmbledhjet afatgjata.

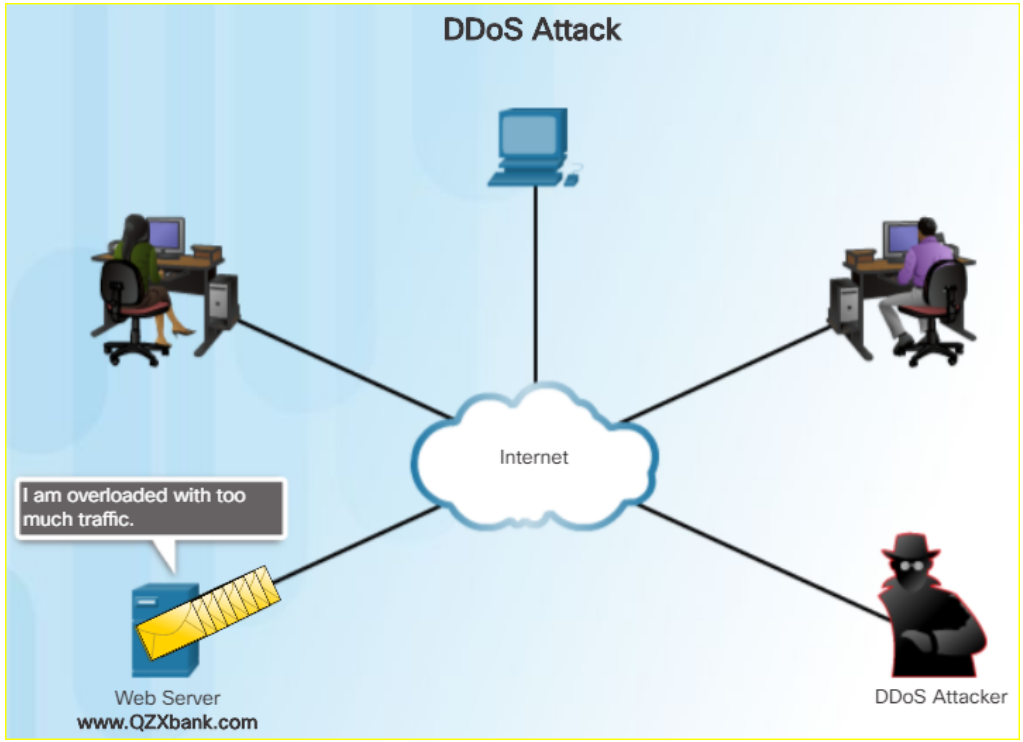
Hyrje në mjetet e monitorimit të rrjetit
Sistemet SIEM

- Splunk është një nga sistemet më popullore SIEM të përdorura nga Qendrat e Operimit të Sigurisë.
- Si një opsion me burim të hapur, ky model përdor suitën ELK për funksionalitetin SIEM. ELK është një akronim për tri produkte me burim të hapur nga Elastic:
- Elasticsearch - Motori i kërkimit me tekst të orientuar drejt dokumentit
- Logstash - Sistemi i përpunimit të tubacionit që lidh "inputet" me "daljet" me "filtrat" opsionale në mes
- Kibana - Analizat e bazuara në shfletues dhe pultet e kërkimit për Elasticsearch

Rreziqet dhe kërcënimet

Sulmet DoS

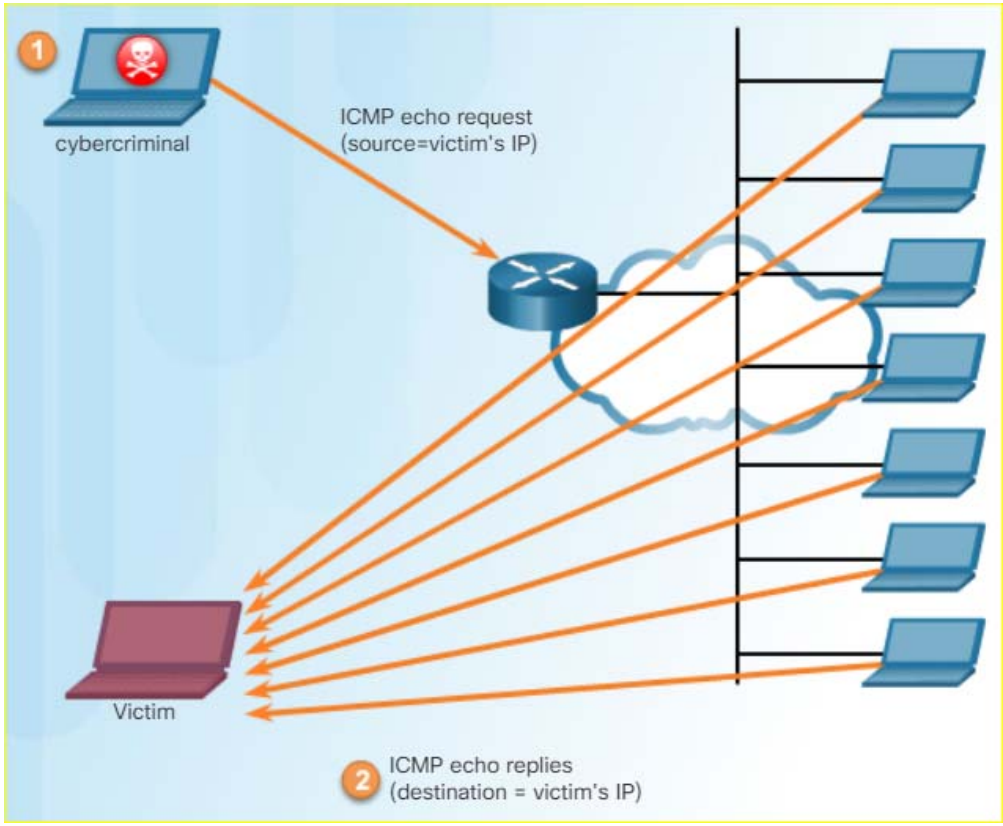
- Qëllimi i një sulmi kundër Denial of Service (DOS) është parandalimi i përdoruesve të ligjshëm nga qasja në faqet e internetit, emailet, llogaritë në internet dhe shërbimet e tjera.
- Ka dy burime kryesore të sulmeve DoS:
  - Paketat me format të dëmtuar - Sulmuesit krijojnë një paketë të formatuar me qëllim të keq dhe e përcjellin atë në një host të prekshëm, duke shkaktuar rrëzimin e hostit ose duke u bërë shumë i ngadalshëm.
  - Sasitë e shumta të trafikut - Akterët e kërcënimit trullosin një rrjet të synuar, host, ose aplikacion, duke i shkaktuar ato të rrëzohen ose të bëhen jashtëzakonisht të ngadalta.
- Sulmi i shpërndarë DoS (DDoS) kombinon sulme të shumta DoS.



Rreziqet dhe kërcënimet

Sulmet e amplifikuara dhe reflektimet

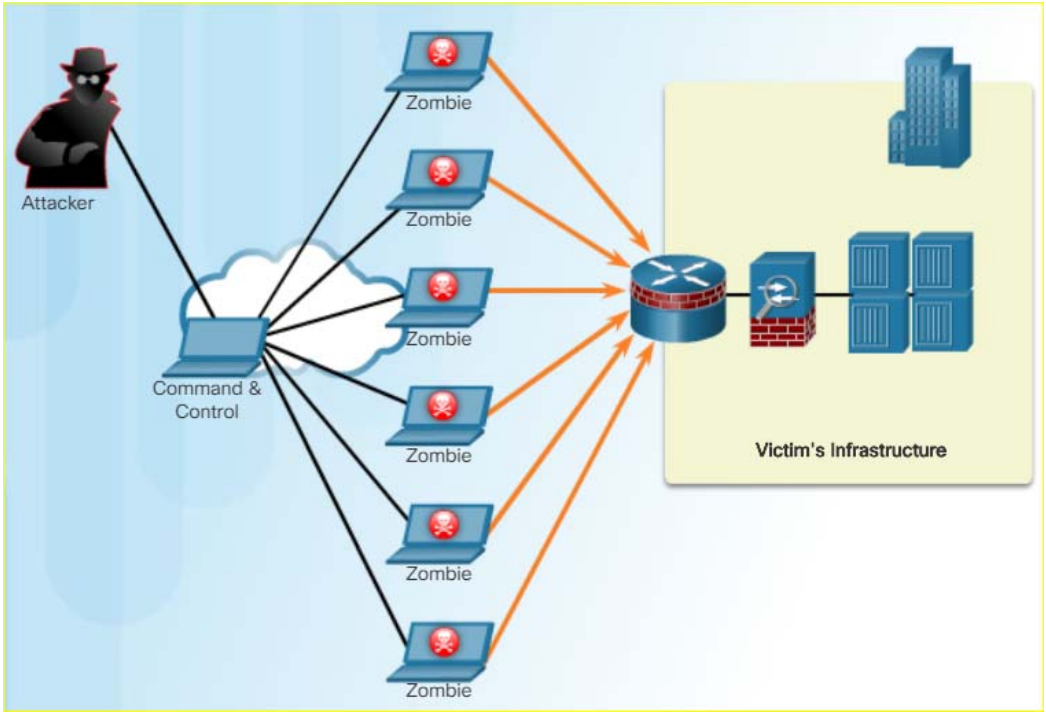
- Sulmuesit shpesh përdorin teknikat e përforcimit dhe të reflektimit për të krijuar sulme DoS. Shembulli në figurën ilustron se si një teknikë për përforcim dhe reflektim të quajtur Sulm Smurf përdoret për të mbytur një host të synuar:
- 1. Zgjerimi - Aktori i kërcënimit përcjell ICMP echo kërkesën dhe mesazhe që përmbajnë adresën IP burimore të viktimës në një numër të madh të ushtrive.
- 2. Reflektim - Keto mbajne te gjithe pergjigjen ne IP adresen te viktimes per ta tronditur ate.



Sulmet e amplifikimit dhe reflektimit

Sulmet DDoS

- Sulmi DDoS është më i madh se një sulm i DoS, sepse ai buron nga burime të shumëfishta dhe të koordinuara.



Shërbimet e Ndërmarrjeve

HTTP dhe HTTPS

- Shfletimi i Webit është ndoshta vektori më i madh i sulmit. Analistët e sigurisë duhet të kenë njohuri të hollësishme se si funksionojnë sulmet në internet.
- IFrames - një iFrame lejon që një faqe nga një fushë tjetër të hapet brenda në faqen aktuale. IFrame mund të përdoret për të nisur kodin e dëmshëm.
- HTTP 302 cushioning - lejon një faqe interneti për të përcjellë dhe hapur në një URL të ndryshme. Mund të përdoret për të ridrejtuar në kodin e dëmshëm.
- Domain shadowing - faqet e internetit me qëllim të keq krijohen nga nënndomeinat e krijuar nga një fushë e tjeter.

Shërbimet e Ndërmarrjeve

Email

- Mesazhet me email arrihen nga shumë pajisje të ndryshme që shpesh nuk mbrohen nga firewall i kompanisë.
  - Attachment-based attacks - email me fotografi të ekzekutueshme e bashkangjitur me qëllim të keq .
  - E-mail spoofing - sulm phishing ku mesazhi duket se vjen nga një burim i ligjshëm.
  - Spam email - email me reklama ose përmbajtje me qëllim të keq.
  - Serveri i hapur i postës - sasi masive e spamit dhe krimbave mund të dërgohen nga serverat e email-it të keqpërcaktuar.
  - Homoglyphs â € "skema e phishing kur karakteret e tekstit (hyperlinks) duken të ngjashme me tekstin dhe lidhjet reale.

Shërbimet e Ndërmarrjeve

Bazat e të dhënave të ekspozuara në ueb

- Aplikacionet në internet zakonisht lidhen me një bazë të dhënash relacionale. Për shkak se bazat e të dhënave relacionale shpesh përmbajnë të dhëna të ndjeshme, bazat e të dhënave janë një objektiv i shpeshtë për sulmet.
  - Sulmet e injektimit të komandës - kodet e pasigurta dhe aplikacioni i uebit lejon që komandat OS të injektohen në fushat e formës ose në shiritin e adresave.
  - XSS Cross-site scripting attacks - insecure server-side scripting ku hyrja nuk është e vlefshme lejon komandat e shkrimit të futen në fusha të formave të krijuara nga përdoruesit, si komentet e faqes së internetit.
    Kjo rezulton që vizitorët janë ridrejtuar në një faqe interneti me qëllim të keq me kodin malware.
  - Sulmet SQL injektimit - skriptimi i pasigurt në serverë lejon që komandat SQL të futen në fushat e formës ku futja nuk është e vërtetuar.
  - Sulmet e injektimit HTTP - manipulimi i html lejon që kodi i ekzekutueshëm të injektohet përmes etiketave të HTML, etj.

Përmbledhje

- Të gjitha rrjetet janë objektiva dhe duhet të sigurohen duke përdorur një qasje mbrojtëse në thellësi.
- Mjetet e përdorura për të ndihmuar në zbulimin e sjelljes normale të rrjetit përfshijnë IDS, analizuesit e paketave, SNMP, NetFlow dhe të tjerët.
- Një rrëshqitje rrjetëzon përpara çdo trafiku duke përfshirë gabimet fizike të shtresës në një pajisje.
- Mirëmbajtja e portit mundëson kalimin në kornizat e një ose më shumë porteve në një port të Analizuesit të Portës së Lidhjes (SPAN) të lidhur me një pajisje analize.
- Analistët mund të përdorin analiza të protokollit si Wireshark dhe tcpdump për të parë shkëmbimet e rrjetit deri në nivelin e paketës.
- NetFlow mund të përdoret për monitorimin e rrjetit dhe sigurisë, planifikimin e rrjetit dhe analizën e trafikut; megjithatë, ai nuk kap përmbajtjen.
- Sistemet e Menaxhimit të Eventeve të Informacionit të Sigurisë (SIEM) sigurojnë raportim në kohë reale dhe analiza afatgjate të ngjarjeve të sigurisë.
- Splunk dhe ELK janë dy sisteme në kuader te SIEM të përdorura nga Qendrat e Operimit të Sigurisë.

Përmbledhje

- Analistët e sigurisë duhet të kuptojnë fusha të ndryshme në të dyja IPv4 dhe IPv6 headers sepse Sulmuesit mund të ngacmojnë informacionin e paketës.
- Ekzistojnë 10 fusha në kokën e paketës IPv4: Version, gjatësia e Internet header, shërbimet e diferencuara ose DiffServ (DS), gjatësia totale, identifikimi, kompensimi i flamurit dhe fragmentit, koha për të jetuar (TTL), protokoll, Adresa IPv4, Adresa IPv4 e destinacionit, Mundësitë e zgjedhjes dhe mbushja.
- Ekzistojnë 8 fusha në kokën e paketës IPv4: Version, Klasa e Trafikut, Etiketa e Fluksit, Gjatësia e Shitjes, Shefja e Tjetra, Kufizimi i Hopit, Adresa e Burimit IPv6, Adresa e Destinacionit IPv6
- Dobësitë e IP përfshijnë sulmet ICMP, sulmet DoS dhe DDoS, spoofing adresa, sulmet MITM, dhe rrëmbimi seanca.
- ICMP është zhvilluar për të kryer mesazhe diagnostike dhe për të raportuar gjendjen e gabimit kur rrugët, pret dhe portet nuk janë të disponueshme. Mesazhet ICMP gjenerohen nga pajisjet kur ndodh një gabim në rrjet ose ndërprerje.

Përmbledhje

- Qëllimi i një sulmi të Denial of Service (DoS) është parandalimi i përdoruesve të ligjshëm nga qasja në faqet e internetit, email, llogaritë në internet dhe shërbimet e tjera.
- Sulmuesit shpesh përdorin teknikat e amplifikimit dhe të reflektimit për të krijuar sulme DoS.
- Një sulm DDoS është më i madh se një sulm i DoS sepse ajo buron nga burime të shumta. Sulmet DDoS prezantuan terma të tillë si botnet, sistemet e mbajtësve dhe kompjuterët mumje.
- Sulmet spoofing të adresës IP ndodhin kur një aktor kërcënimi krijon paketa me informacion të adresave IP të burimit të rremë ose fsheh identitetin e dërguesit ose paraqet si një përdorues tjetër legjitim.
- TCP ofron shërbimet e mëposhtme: shpërndarjen e besueshme, kontrollin e rrjedhës, komunikimin e gjendjes.
- Edhe pse protokoli TCP është një protokoll i orientuar drejt lidhjes dhe i besueshëm, ka ende dobësi që mund të shfrytëzohen.
- UDP është një protokoll i thjeshtë që siguron funksionet bazë të shtresave të transportit. UDP zakonisht përdoret nga DNS, TFTP, NFS dhe SNMP. Ajo përdoret gjithashtu edhe me aplikacione në kohë reale si media streaming ose VoIP. UDP është një protokoll i lidhjes së transportit pa lidhje.

Përmbledhje

- Pret transmeton një kërkesë ARP për hostë të tjerë në segment për të përcaktuar adresën MAC të një host me një adresë IP të veçantë.
- Sulmet me helmim të ARP në mënyrë të qëllimshme helmojnë cache-in e një kompjuteri tjetër me adresë IP të spoofed në mappings adresën MAC.
- Serverët DNS zgjidhin emrat në adresat IP dhe janë një objektiv i madh i sulmuesve.
- Kërcënuesit të cilët përdorin DNS tunneling vendosin trafikun jo-DNS brenda trafikut DNS.
- Një sulm DHCP spoofing krijon një server DHCP mashtrues për të shërbyer informacion të falsifikuar.
- Shfletimi i Web (http dhe https) është ndoshta vektori më i madh i sulmit. Analistët e sigurisë duhet të kenë njohuri të hollësishme se si funksionojnë sulmet në internet.
- Mesazhet me email arrihen nga shumë pajisje të ndryshme që shpesh nuk mbrohen nga firewall i kompanisë.
- Aplikacionet në internet zakonisht lidhen me një bazë të dhënash relacionale. Për shkak se bazat e të dhënave relacionale shpesh përmbajnë të dhëna të ndjeshme, bazat e të dhënave janë një objektiv i shpeshtë për sulmet.